NAC 4.5 : Exemple de configuration d'Import-Export de stratégie

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Le NAC configurent](#)
[Vérifiez](#)
[Dépannez](#)
[Se connecter](#)
[Questions](#)
[Informations connexes](#)

Introduction

Ce document fournit un guide pas à pas sur la façon dont configurer la caractéristique de Policy Import Export (SECTEUR) sur la version 4.5 de Cisco NAC. Le but de cette caractéristique est de synchroniser les filtres de périphérique, les règles du trafic et de correction, et les profils de port entre les gestionnaires NAC (gestionnaires de Clean Access). Quand cette caractéristique est discutée, le gestionnaire NAC où des stratégies sont définies s'appelle le **maître**, qui peut pousser ou synchronise les stratégies de l'autant d'en tant que dix gestionnaires NAC (gestionnaires de Clean Access), appelé **Receivers**. Des stratégies peuvent être synchronisées automatiquement avec un temporisateur de présélection ou par un sync manuel.

Conditions préalables

Cisco recommande que vous ayez la connaissance de l'interface web de gestionnaire de Cisco NAC (Clean Access Manager) et les stratégies qui sont typiquement configurés. Référez-vous aux notes en version pour la version 4.5 de Cisco NAC pour des informations sur ce qui est pris en charge et pas pris en charge avec le SECTEUR.

Conditions requises

Installez les gestionnaires et les serveurs NAC selon le guide d'installation et de configuration de Cisco NAC. Référez-vous aux recommandations de pratique recommandée pour configurer le Policy Import Export de gestionnaire NAC afin d'identifier quel gestionnaire doit être utilisé comme maître et lesquels comme récepteur. Ce document suppose que les gestionnaires de maître et de récepteur NAC sont identifiés et les recommandations de pratique recommandée sont utilisées.

Composants utilisés

Les informations dans ce document sont basées sur le logiciel 4.5.0 de Cisco NAC.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

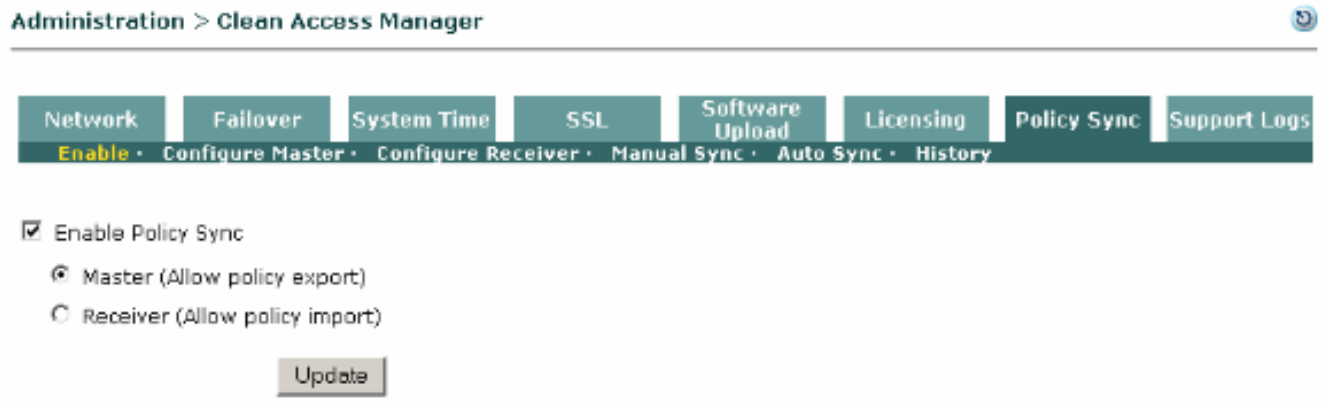
Remarque: Avant que vous commenciez, confirmez que le maître et les récepteurs exécutent le précis les mêmes versions. En outre, assurez-vous que les configurations de mise à jour de Ruleset sous la **Gestion de périphériques > le Clean Access > met à jour >** correspondance de **mise à jour** sur le maître et tous récepteurs.

Le NAC configurent

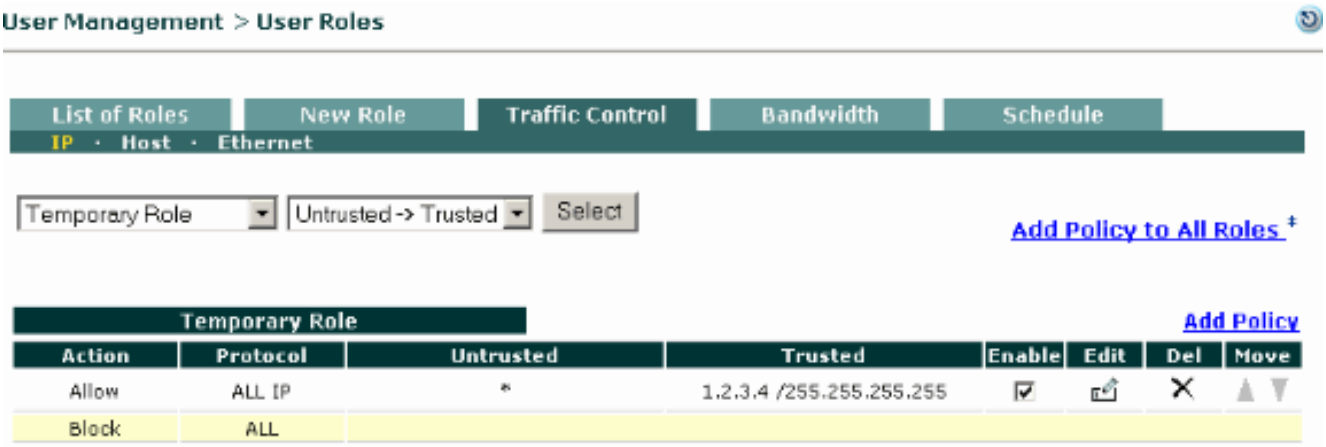
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Terminez-vous ces étapes afin de configurer l'importation/exportation de stratégie entre les gestionnaires NAC.

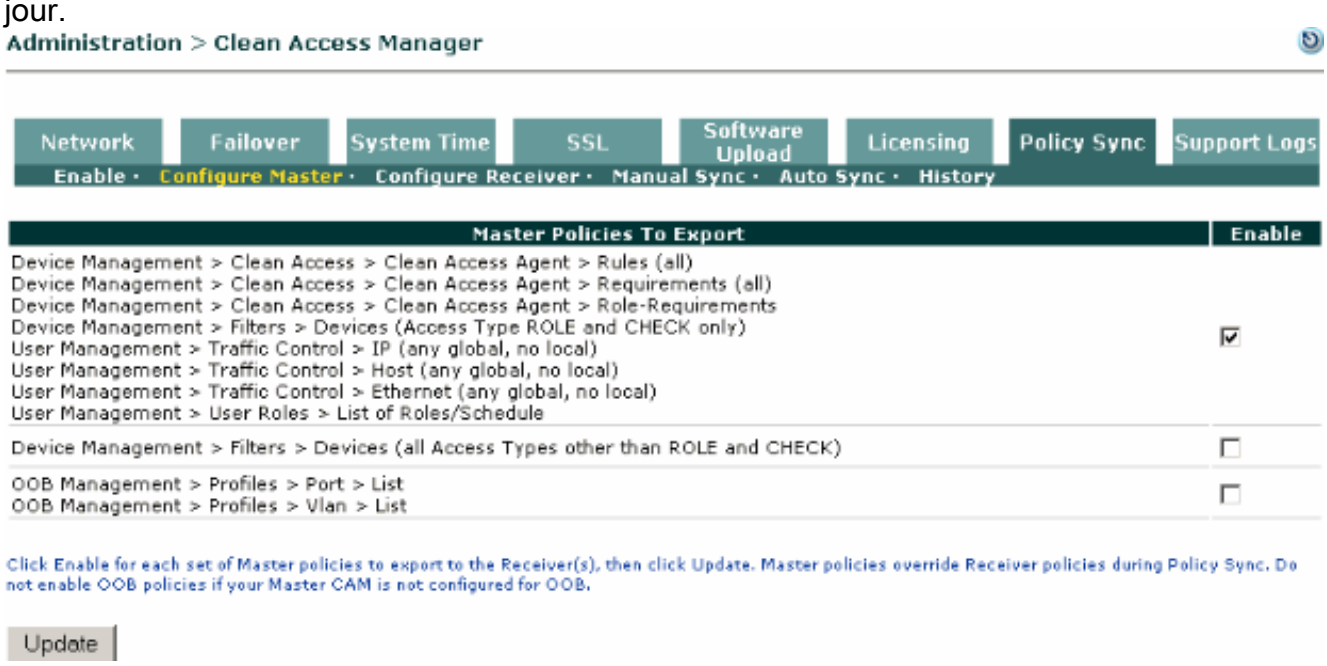
1. **Sync de stratégie d'enable sur le gestionnaire principal NAC :**Sur le gestionnaire du maître NAC, naviguez vers la gestion > le gestionnaire de CCA > le sync > l'enable de stratégie.



   Cochez la case de **sync de stratégie d'enable**. Choisissez **(permettez l'exportation de stratégie) l'**option **principale**, et cliquez sur la **mise à jour**.
2. **Identifiez les stratégies à pousser :**Dans cette étape, vous identifiez les stratégies qui doivent être synchronisées entre le CAM principal et les récepteurs. Pour cet exemple, le but est de synchroniser les stratégies de contrôle de trafic globales entre les gestionnaires. Dans ce cas, la stratégie de trafic basée sur IP globale doit être choisie sous les rôles de l'utilisateur > le contrôle de trafic > l'IP (le rôle provisoire choisi, non approuvé > a fait confiance dans la baisse vers le bas, comme affiché. Clic choisi. Cette règle n'existe pas sur le récepteur encore.

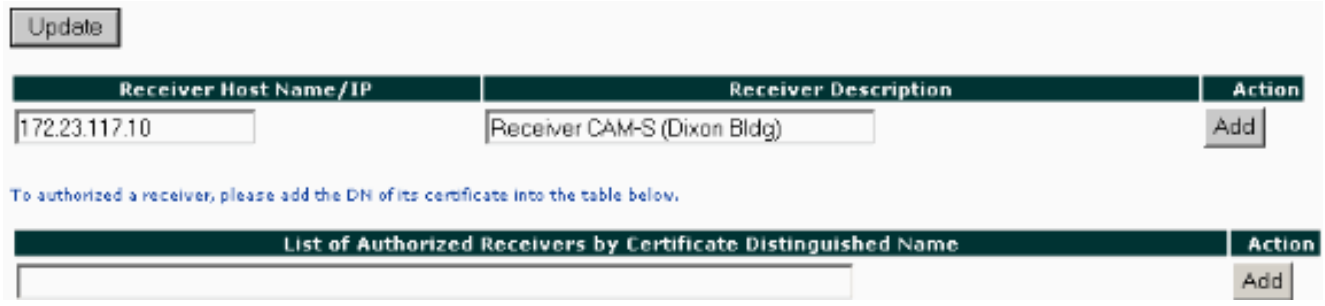


Référez-vous ajoutent des stratégies de trafic basées sur IP globales pour les informations sur la façon dont configurer des stratégies du trafic IP.Choisissez la gestion > le Clean Access Manager > le sync de stratégie > configurent le maître et cochent la case d'enable comme affiché et cliquent sur la mise à
jour.

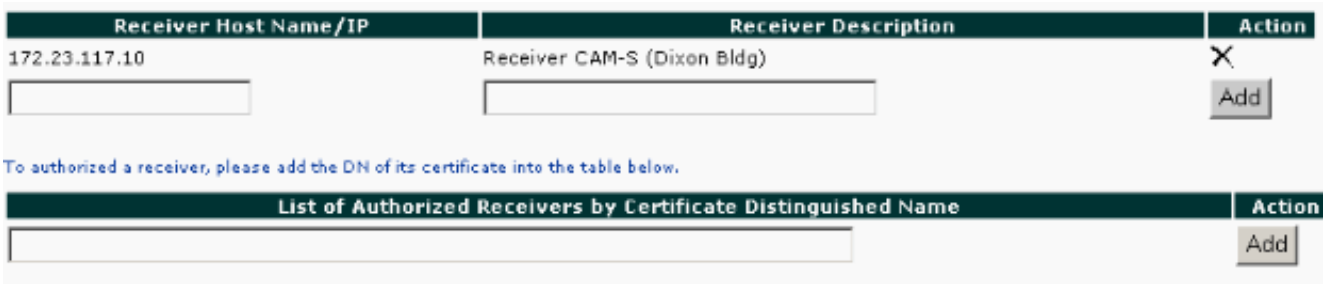


Remarque: Synchroniser le trafic maintient l'ordre exige également synchroniser des règles, des conditions requises, des conditions requises de rôle, des filtres de périphérique (des types de RÔLE, de CONTRÔLE) et des rôles.

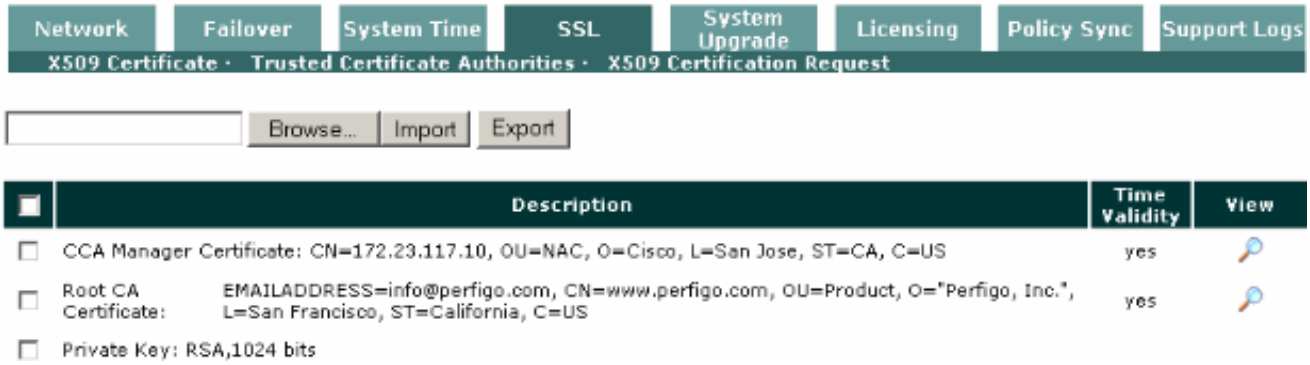
3. **Ajoutez/identifiez les récepteurs :**Vous pouvez ajouter à dix récepteurs pris en charge à votre maître. Dans cet exemple, vous ajoutez un récepteur au gestionnaire du maître NAC.Choisissez la gestion > le Clean Access Manager > le sync de stratégie > configurent le maître. Sous l'hôte Name/IP de récepteur, ajoutez l'adresse Internet (le gestionnaire de maître le NAC doit pouvoir résoudre des DN pour le nom d'hôte) ou l'adresse IP du récepteur. Ajoutez une description facultative et cliquez sur
Add.



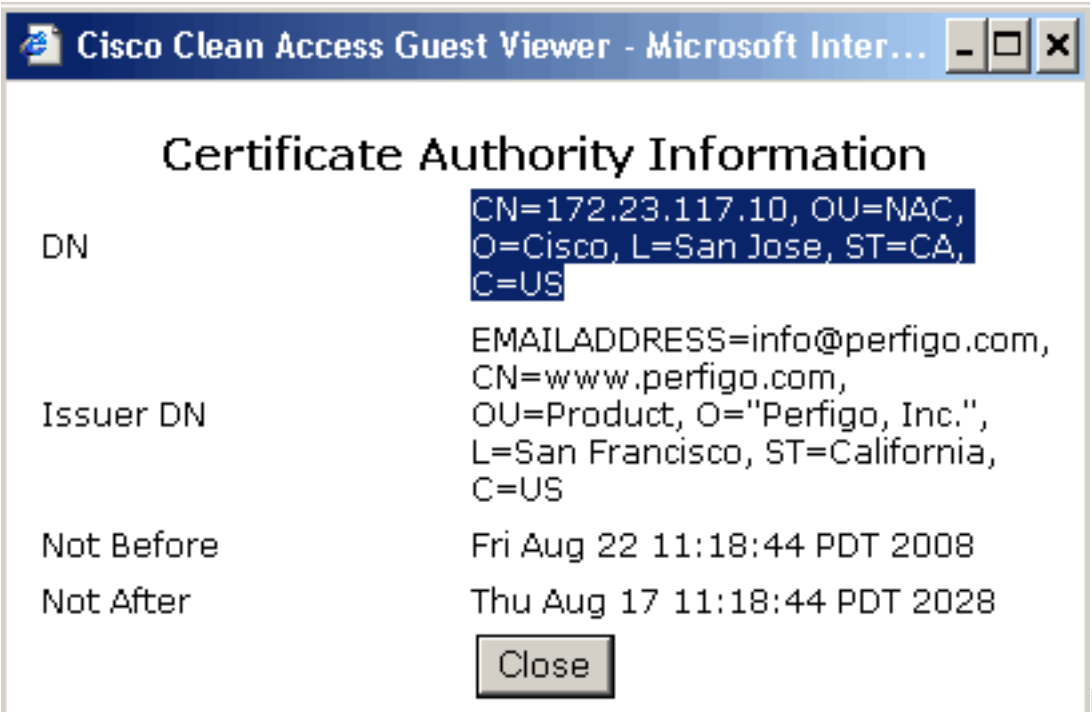
Une fois qu'ajouté, le nouveau récepteur apparaît. Vous pouvez ajouter les plusieurs récepteurs (jusqu'à dix pris en charge) de cette façon. Dans les scénarios (ha) facilement disponibles, vous devez ajouter nom d'hôte virtuel/partagé ou adresse IP virtuelle/partagée des paires ha à la
liste.



4. **Autorisez les récepteurs :**Après que vous ajoutiez les récepteurs, il est important de sécuriser la transmission entre le maître et les récepteurs. Seulement un maître autorisé peut pousser des stratégies à un récepteur. De même, le maître doit pouvoir communiquer seulement avec les récepteurs autorisés. En outre, une confiance doit être établie pour s'assurer que le maître et les récepteurs sont qui ils prétendent être. Le SSL est utilisé à cet effet. Non seulement le maître et le récepteur doivent-ils s'identifier par les informations de DN dans le certificat, mais ils doivent également avoir leur certificat d'identité d'une autorité de confiance (CA). Dans le besoin court, principal et de récepteur de faire confiance aux Certificats de chacun.Puisque ce document est généré d'une installation de laboratoire, des Certificats auto-signés sont utilisés dans cet exemple. Cependant, notez que vous devez utiliser un certificat signé CA dans votre environnement de production. Référez-vous aux recommandations de pratique recommandée pour configurer le pour en savoir plus de Policy Import Export de gestionnaire NAC.Sur le récepteur, choisissez la gestion > le gestionnaire de CCA > le certificat SSL >
X509.



Identifiez le certificat de gestionnaire de CCA et cliquez sur en fonction l'icône sous la vue. Dans la fenêtre qui apparaît, sélectionnez et copiez (clic droit et copie) les informations de

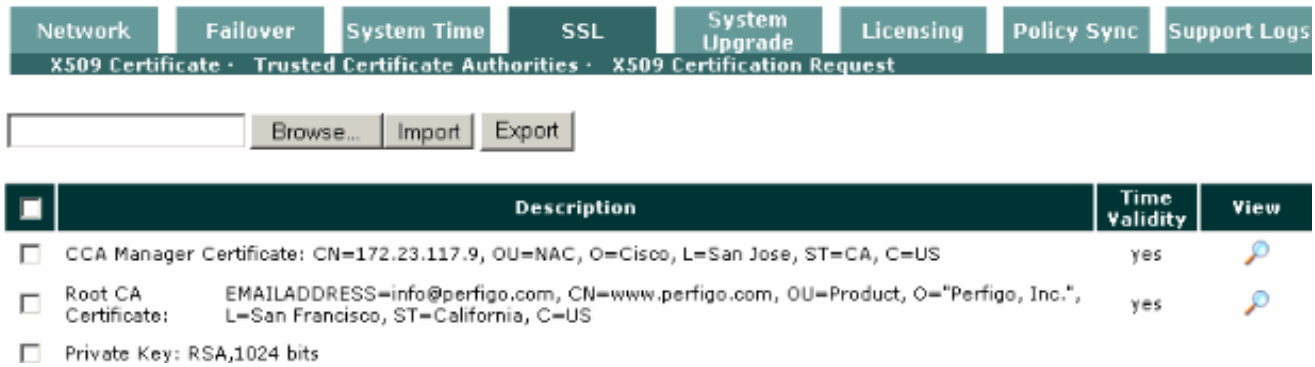


DN. Le retour au gestionnaire du maître NAC sous la gestion > le gestionnaire de CCA > le sync de stratégie > configurent le maître. Au bas, sous la liste de récepteurs autorisés par le nom unique de certificat, pâte les informations de DN de certificat que vous avez copiées du récepteur dans l'étape précédente et cliquez sur
Add.

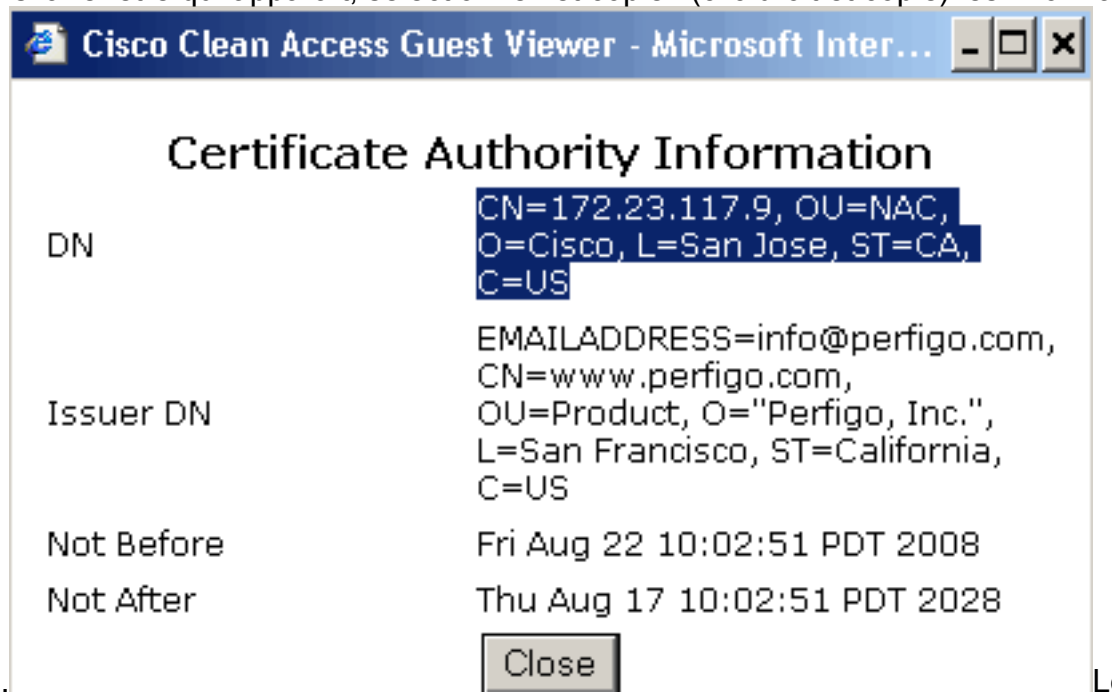
5. **Sync de stratégie d'enable sur le gestionnaire du récepteur NAC :**Sur le gestionnaire du récepteur NAC, naviguez vers la gestion > le gestionnaire de CCA > le sync > l'enable de stratégie.Cochez la case de **sync de stratégie d'enable**. Choisissez l'option de **récepteur (permettez l'importation de stratégie)**, et cliquez sur la **mise à jour**.**Remarque:** Notez que la bannière sur le dessus tourne le rouge, qui indique que ce gestionnaire NAC est activé être un
récepteur.

6. **Autorisez le maître :**Sur le maître, choisissez la gestion > le gestionnaire de CCA > le certificat SSL >

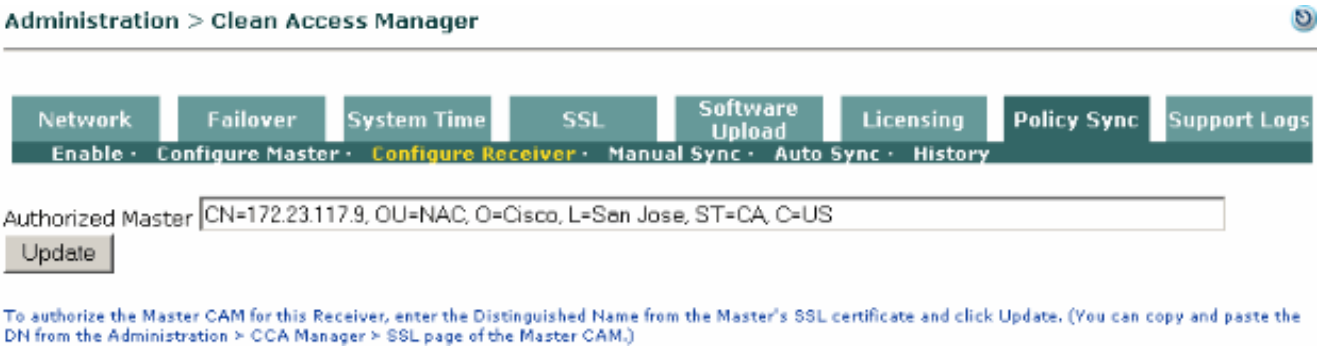
X509.



Identifiez le certificat de gestionnaire de CCA et cliquez sur en fonction l'icône sous la vue. Dans la fenêtre qui apparaît, sélectionnez et copiez (clic droit et copie) les informations de DN.

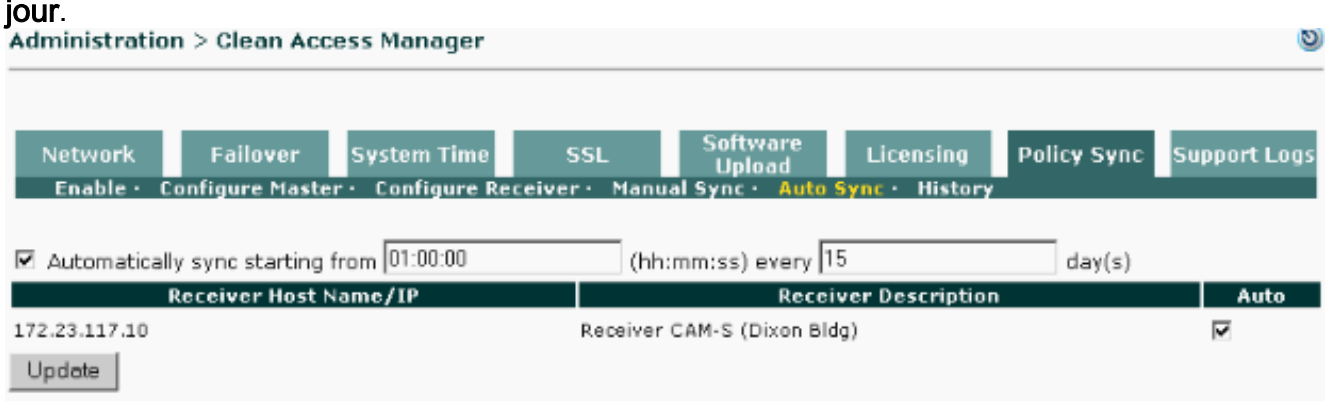


Le retour au gestionnaire du récepteur NAC sous la gestion > le gestionnaire de CCA > le sync de stratégie > configurent le récepteur. À côté du maître autorisé, collez les informations de DN de certificat que vous avez copiées du maître dans l'étape et la mise à jour précédentes de clic.



7. **Configurez le sync automatique (facultatif) :**Le sync de stratégie peut être manuel ou a automatisé. Un sync manuel peut être exécuté sur un suivant les nécessités, alors qu'un temporisateur automatique de sync peut être installé pour exécuter automatiquement un sync de stratégie entre les gestionnaires NAC une fois chaque nombre *x de* jours (le minimum est d'un jour) à un temps prédéterminé. Cisco vous recommande vivement exécutent un sync manuel et le vérifient que le sync fonctionne avec succès avant que vous activiez le sync automatique entre vos gestionnaires NAC. Voyez pour dépanner afin de comprendre comment vous pouvez employer le sync manuel pour dépanner le problème lié

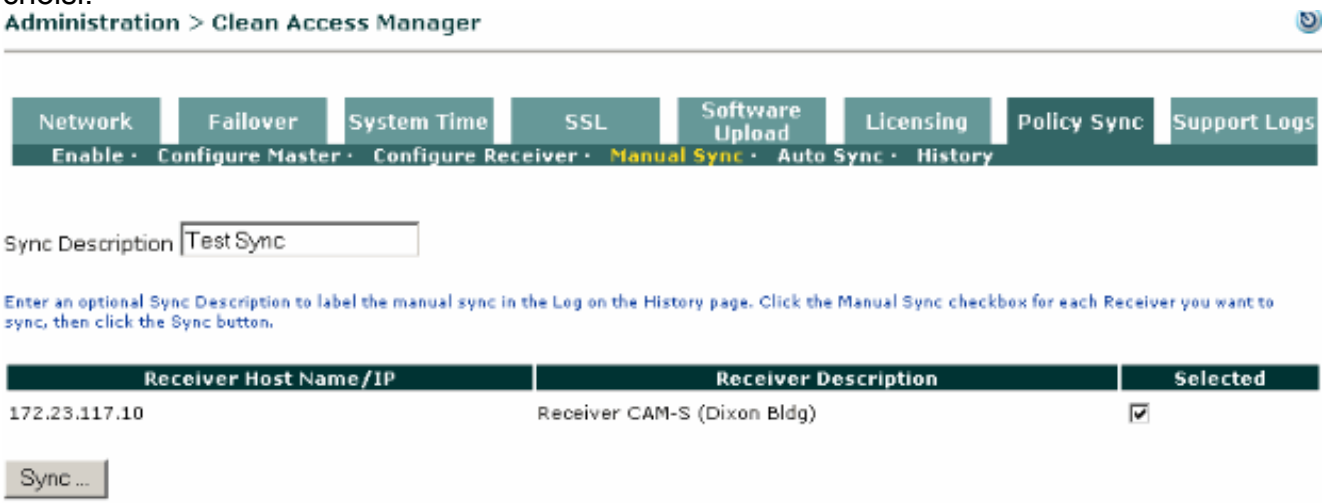
au SECTEUR.Afin d'activer le sync automatique, naviguez vers la gestion > le gestionnaire de CCA > le sync de stratégie > sync automatique sur le gestionnaire du maître NAC.Vérifiez **automatiquement le sync à partir du _(hh : millimètre : solides solubles) chaque** case de **jours de** _.Écrivez la période du sync (1:00 AM dans cet exemple) et combien de fois (tous les 15 jours dans cet exemple) ce vous voulez exécuter le sync automatique.Cochez la case sous l'**automatique** afin de sélectionner les récepteurs qui reçoivent automatiquement des stratégies sur une base périodique, et cliquez sur la **mise à jour**.



Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

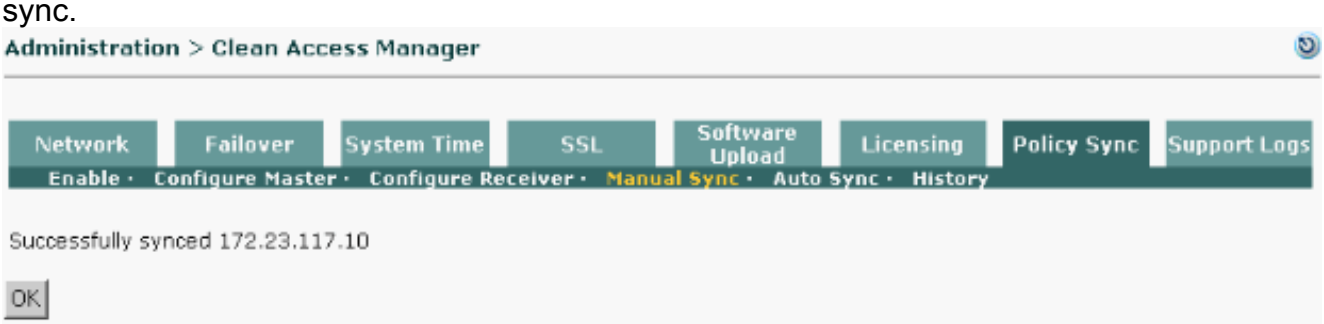
1. Naviguez vers la gestion > le gestionnaire de CCA > le sync de stratégie > sync manuel sur le maître.
2. Introduisez un nom (facultatif) pour la synchronisation sous la description de sync
3. Sélectionnez les récepteurs sur lesquels vous voulez exécuter l'action de sync. Cochez la case sous sélectionné, et cliquez sur le **sync**. Dans cet exemple, vous avez seulement un récepteur, 172.23.117.10, ainsi il est choisi.



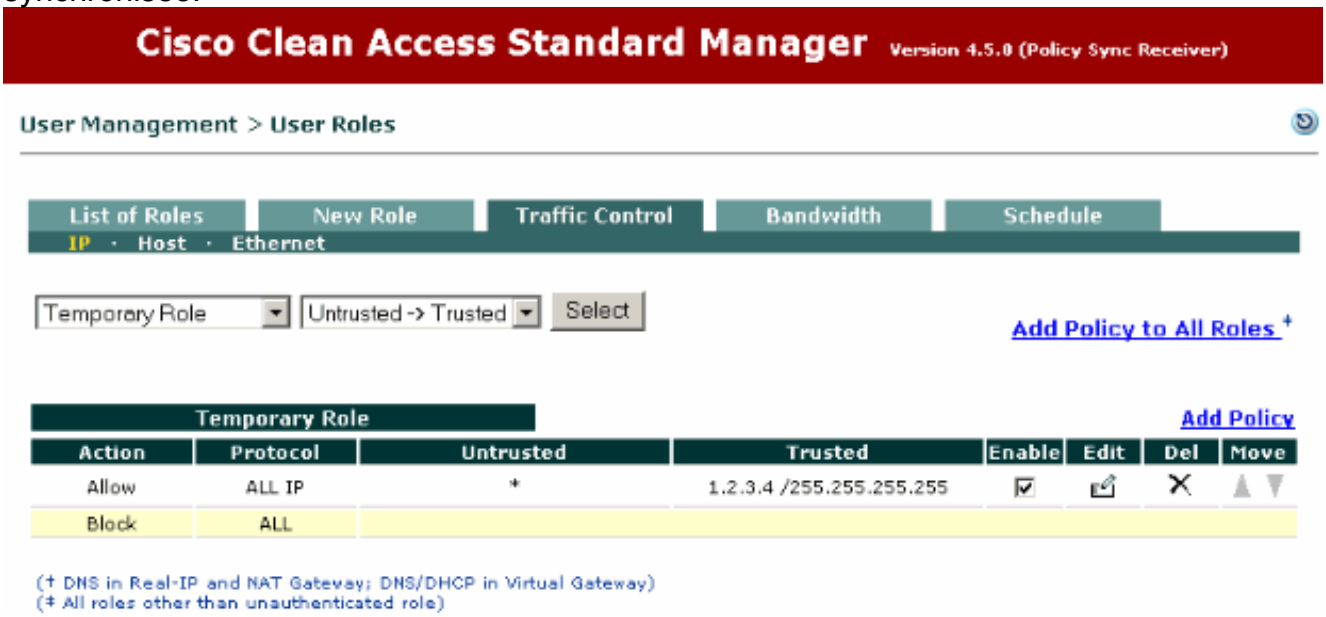
4. En ce moment, le maître exécute un contrôle de validité de pré-sync contre le récepteur. Le contrôle de pré-sync s'assure que les gestionnaires de maître et de récepteur NAC sont configurés correctement (pour pousser et recevoir des stratégies), et que les informations d'autorisation sont correctes, etc. S'il y a de la configuration ou erreurs d'autorisation, le contrôle de pré-sync échoue avec les messages d'erreur appropriés. Voyez la section de dépannage.
5. S'il n'y a aucune question de configuration ou d'autorisation, le maître affiche un contrôle

réussi de pré-
sync.

6. Le hit continuent à se terminer avec succès le
sync.



7. Allez au gestionnaire du récepteur NAC et vérifiez que la règle de la circulation est synchronisée.



Dépannez

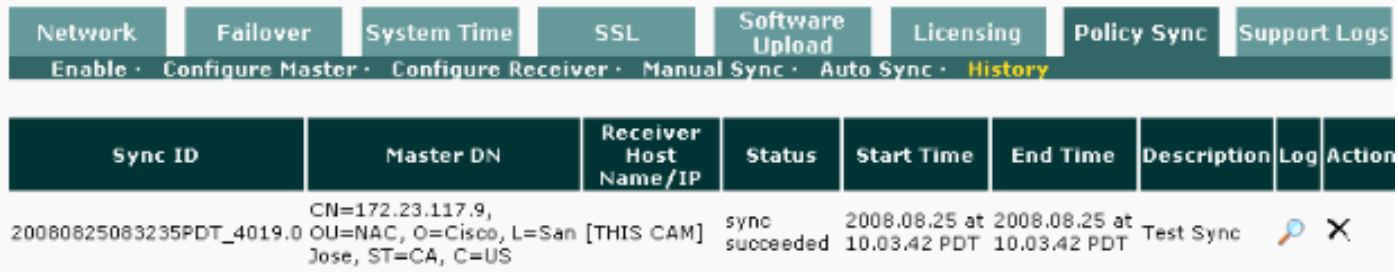
Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Se connecter

Le résumé de sync est enregistré sous le gestionnaire de CCA > le sync > l'historique de stratégie sur le maître et les récepteurs.

Sur le gestionnaire du maître NAC :

Sur le gestionnaire du récepteur NAC :



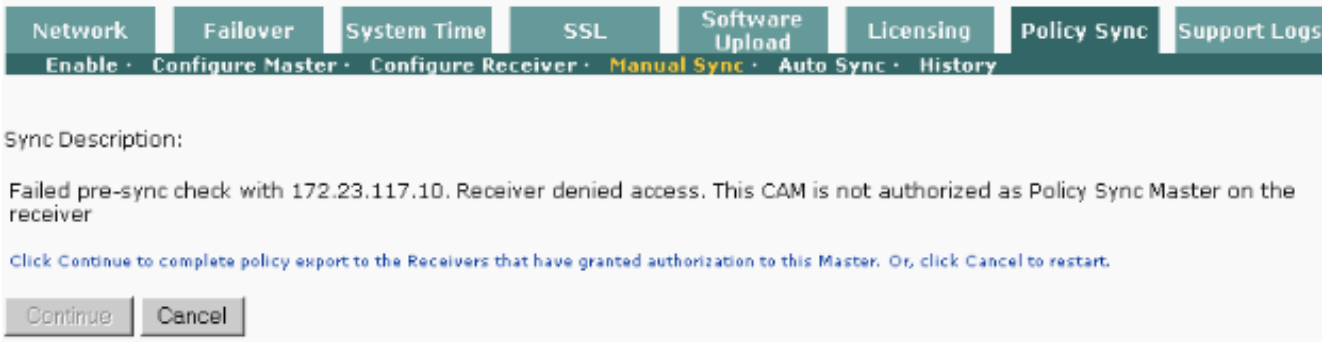
Cliquez sur l'icône de loupe sous la commande de procédure de connexion pour visualiser les logs de transaction détaillés :

```
*************** Master Log ***************

Starting policy import/export on Policy Sync Master.
Created dump file for policy: User Management -> User Roles -> List of Roles/Schedule
Created dump file for policy: Device Management > Clean Access > Clean Access Agent > Role-
Requirements
Created dump file for policy: Device Management > Filters > Devices
Created dump file for policy: User Management->Traffic Control->IP
Created dump file for policy: User Management->Traffic Control->Host
Created dump file for policy: User Management->Traffic Control->Ethernet
Dump file creation is complete.
Created policy import/export dump file.
Created  policy import/export header file.
Created policy import/export tar file.


*************** Receiver Log ***************

Starting policy import on Policy Sync Receiver.
Hash value is a match.
Policy Sync Master and Receiver CAM versions match.
All SQL statements successfully executed
All requirements are valid.
All rules are valid.
Role tables integrity check is successful.
```

L'importation/exportation de stratégie s'est avec succès terminée sur le récepteur de sync de stratégie.

Questions

1. **Accès refusé par récepteur. Ce CAM n'est pas autorisé en tant que maître de sync de stratégie sur le récepteur.**

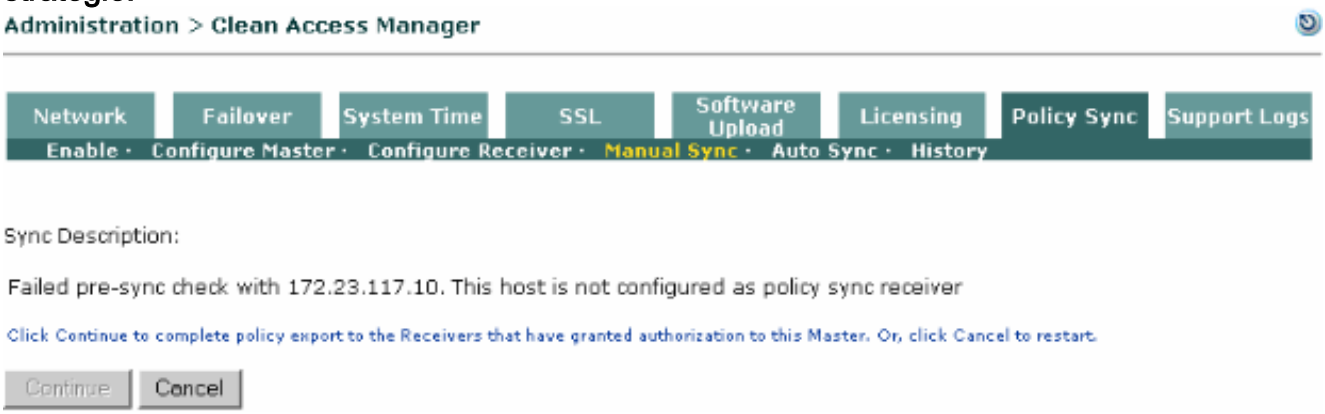


Cette erreur signifie typiquement que le récepteur rejette le sync de stratégie parce que les informations principales de DN misconfigured sur le gestionnaire du récepteur NAC. Choisissez la gestion > le gestionnaire de CCA > le sync de stratégie > configurent le récepteur sur le récepteur et s'assurent que » les informations principales « autorisées sont configurées correctement.

2. **Ce récepteur n'est pas autorisé**

Ce message signifie typiquement que le récepteur n'est pas installé pour l'autorisation ou les paramètres d'autorisation (les informations du DN du récepteur) configurés sur le gestionnaire du maître NAC est incorrect. Choisissez la gestion > le gestionnaire de CCA > le sync de stratégie > configurent le maître sur le maître et s'assurent que les informations de DN du certificat du récepteur existent sous la liste de récepteurs autorisés par le nom unique de certificat et sont configurées correctement.

3. **Cet hôte n'est pas configuré en tant que récepteur de sync de stratégie.**



Ce message signifie typiquement que les essais de maître au sync à un hôte qui ou n'est pas activé pour le sync de stratégie ou il n'est pas configurés pour être un récepteur. Choisissez la gestion > le gestionnaire de CCA > le sync > les configurations de stratégie sur le gestionnaire NAC qui est choisi pour être le récepteur et pour s'assurer que la case activée par sync de stratégie est cochée et que la case d'option est placée au récepteur

(permettez importer la stratégie).

Informations connexes

- Support et documentation techniques - Cisco Systems